

シナリオ:IPSec リモートアク セス VPN 設定

この章では、適応型セキュリティアプライアンスを使用して、リモートアクセス IPsec VPN 接続を受け入れる方法について説明します。リモートアクセス VPN を使用すると、インターネットを越えてセキュアな接続(トンネル)を作成でき、オフサイトのユーザにセキュアなアクセスを提供できます。

Easy VPN ソリューションを実装する場合、この章では、Easy VPN サーバ(別 名、ヘッドエンドデバイス)を設定する方法について説明します。

この章には、次の項があります。

- IPSec リモートアクセス VPN ネットワーク トポロジの例 (7-2 ページ)
- IPSec リモートアクセス VPN シナリオの実装(7-3ページ)
- 次の作業(7-24ページ)

IPSec リモートアクセス VPN ネットワーク トポロジの例

図 7-1 に、インターネットを越えて Cisco Easy VPN ソフトウェア クライアント またはハードウェア クライアントなどの VPN クライアントからの要求を受け入 れ、VPN クライアントとの IPSec 接続を確立するように設定された適応型セキュ リティ アプライアンスを示します。



図 7-1 リモート アクセス VPN シナリオのネットワーク レイアウト

IPSec リモートアクセス VPN シナリオの実装

ここでは、リモート クライアントおよびデバイスから IPSec VPN 接続を受け入 れるように適応型セキュリティ アプライアンスを設定する方法について説明し ます。Easy VPN ソリューションを実装する場合、この項では、Easy VPN サーバ (別名、ヘッドエンドデバイス)を設定する方法について説明します。

設定内容の例で使われる値は、図 7-1 に示すリモートアクセス シナリオのもので す。

この項は、次の内容で構成されています。

- 収集する情報(7-4ページ)
- ASDM の起動 (7-4 ページ)
- IPSec リモートアクセス VPN 用の ASA 5505 の設定(7-6ページ)
- VPN クライアント タイプの選択(7-7ページ)
- VPN トンネル グループ名と認証方式の指定(7-9ページ)
- ユーザ認証方式の指定(7-11ページ)
- (オプション) ユーザアカウントの設定(7-13ページ)
- アドレスプールの設定(7-14ページ)
- クライアントアトリビュートの設定(7-16ページ)
- IKE ポリシーの設定(7-18 ページ)
- IPSec Encryption パラメータ および Authentication パラメータの設定 (7-19 ページ)
- アドレス変換の例外およびスプリットトンネリングの指定(7-20ページ)
- リモートアクセス VPN 設定の確認(7-22ページ)

収集する情報

リモート アクセス IPSec VPN 接続を受け入れるように適応型セキュリティ アプ ライアンスを設定する手順を開始する前に、次の情報を手元に用意してください。

- IP プールで使用する IP アドレスの範囲。これらのアドレスは、正常に接続 されると、リモート VPN クライアントに割り当てられます。
- ローカル認証データベースを作成するときに使用するユーザのリスト(認証 用に AAA サーバを使用している場合を除く)。
- VPN に接続する場合に、リモート クライアントが使用するネットワーキング情報。内容は次のとおりです。
 - プライマリおよびセカンダリの DNS サーバの IP アドレス
 - プライマリおよびセカンダリの WINS サーバの IP アドレス
 - デフォルトのドメイン名
 - 認証されたリモート クライアントにアクセスできるローカル ホスト、 グループ、およびネットワークの IP アドレスのリスト

ASDM の起動

Web ブラウザで ASDM を実行するには、アドレス フィールドに工場出荷時のデ フォルト IP アドレス https://192.168.1.1/admin/ を入力します。



i 「https」の「s」を付け忘れると、接続は失敗します。HTTP over SSL(HTTPS) を使用すると、ブラウザと適応型セキュリティアプライアンスとの間の 安全な接続が可能になります。

メイン ASDM ウィンドウが表示されます。

Cisco ASDM 5.2								
File Options Tools Wizards Help				Search:				Find 👻
Home Configuration Monitoring Back Forward	C Packet Tracer	Q Refresh	III Save	? Help				
Device Information		Interface Statu	IS					
General License		Interface	IP Address/	Mask Li	ne	Link	Kbps	
	1	dmz	10.30.30.1/2	24 🗧	down	😑 down	0	
Host Name: SecurityAppliance1		inside	10.10.10.1/2	24 🗧	down	😑 down	0	
ASA Version: 7.2(0)72 Device Uptime: 1d 1h 48m 24	ls 🛛	management	172.23.62.2	2/24	up	🕤 up	5	
ASDM Version: 5.2(0)30 Device Type: ASA/PIX		outside	209.165.200	.225/24 🗧	down	😑 down	0	
Environment and a contract Marian Classic								
Firewaii mode: Routed Context mode: Single								
Total Flash: 64 MB Total Memory: 512 MB		Select an inter	face to view inp	ut and output Ki	ops			
VPN Status		Traffic Status						
IKE Tunnels: 0 WebVPN Tunnels: 0 SVC Tunnels	s: 0	- Connections F	Per Second Usag	e				
-Sistem Resources Status		2	-					
CPU CPU Usage (percent)								
		outside' Interf.	ace Traffic Usag	e (Kbps)				
Memory Memory Line flace is down. 08 1 08 34								
01.08:10 01.03:22 01:05:08 01:06:48 01:08:08 Input Kbps: ■ Output Kbps:								
**								
Device configuration loaded successfully.		<admin></admin>	15	5		6/10/0	6 1:08:18	AM PD

IPSec リモートアクセス VPN 用の ASA 5505 の設定

リモートアクセス VPN の設定用のプロセスを開始するには、次の手順に従います。

ステップ1 ASDM メイン ウィンドウで、Wizards ドロップダウン メニューから VPN Wizard を選択します。VPN Wizard Step 1 画面が表示されます。



ステップ2 VPN Wizard の Step 1 で、次の手順に従います。

- a. Remote Access オプション ボタンをクリックします。
- **b.** ドロップダウン リストから、着信 VPN トンネルで有効なインターフェイス として Outside を選択します。
- C. Next をクリックして続行します。

VPN クライアント タイプの選択

VPN Wizard の Step 2 で、次の手順に従います。

ステップ1 この適応型セキュリティ アプライアンスに接続するリモート ユーザを有効にす る VPN クライアントのタイプを指定します。このシナリオでは、Cisco VPN Client オプション ボタンをクリックします。

その他の Cisco Easy VPN リモート製品も使用できます。

■ IPSec リモートアクセス VPN シナリオの実装

🖆 VPN Wizard	
VPN Wizard	Remote Access Client (Step 2 of)
Branch	Remote access users of various types can open VPN tunnels to this ASA. Select the type of VPN client for this tunnel.
Home	VPN Client Type:
(corporate)	O Cisco VPN Client, Release 3.x or higher.
Network	or other Easy ∀PN Remote product
THE PAR	Microsoft Windows client using L2TP over IPSec
	specified on the remote client, do not specify it.
STAND	PAP VCHAP VMS-CHAP-V1 MS-CHAP-V2 EAP-PROXY
TIT	Specify if the client will send tunnel group name as - username@tunnelgroup.
- 6-	Client will send tunnel group name as username@tunnelgroup.
	If pre-shared authentication is used with this option then DefaultRAGroup's pre-shared key and ppp authentication are also modified.
	< Back Next > Finish Cancel Help

ステップ2 Next をクリックして続行します。

VPN トンネル グループ名と認証方式の指定

VPN Wizard の Step 3 で、次の手順に従います。

- **ステップ1** 次のいずれかの操作を実行して、使用する認証のタイプを指定します。
 - 認証にスタティック事前共有キーを使用するには、Pre-Shared Key オプションボタンをクリックし、事前共有キー(たとえば、「Cisco」)を入力します。このキーは、適応型セキュリティアプライアンス間の IPSec ネゴシエーションで使用されます。
 - 認証にデジタル証明書を使用するには、Certificate オプション ボタンをク リックし、ドロップダウンリストから証明書署名アルゴリズムを選択し、次 に、事前設定されているトラストポイント名をドロップダウン リストから 選択します。

認証にデジタル証明書を使用する予定で、まだトラストポイント名を設定していない場合は、他の2つのオプションのいずれかを使用してウィザードを 続行できます。認証設定は、標準 ASDM ウィンドウを使用して後で修正で きます。

 Challenge/Response Authentication (CRACK) オプション ボタンをクリック すると、この認証方式を使用できます。

薩 VPN Wizard		×
VPN Wizard	VPN Client Authentication Method and Tunnel Group Name (Step 3 of)	
Branch Branch Branch Homo Corporate Network	The ASA allows you to group remote access tunnel users based on common connection parameters and client attributes configured in the subsequent screens. Configure authentication method and tunnel group for this remote connection. Use the same tunnel group name for the device and the remote client.	
	<u>≤Back</u> <u>N</u> ext > Einish <u>Cancel</u> <u>H</u> elp	

- **ステップ2** 共通の接続パラメータおよびクライアント アトリビュートを使用して、この適応型セキュリティ アプライアンスに接続する複数ユーザのセットのトンネル グループ名(たとえば、「Cisco」)を入力します。
- ステップ3 Next をクリックして続行します。

ユーザ認証方式の指定

ユーザの認証は、ローカル認証データベース、または外部の Authentication, Authorization, and Accounting (AAA; 認証、認可、アカウンティング)サーバを使 用して実行できます (AAA サーバには RADIUS、TACACS+、SDI、NT、Kerberos、 および LDAP があります)。

VPN Wizard の Step 4 で、次の手順に従います。

- **ステップ1** 適応型セキュリティ アプライアンスにユーザ データベースを作成してユーザを 認証するには、Authenticate Using the Local User Database オプション ボタンを クリックします。
- **ステップ2** 外部 AAA サーバ グループを使用してユーザを認証する場合は、次の手順に従い ます。
 - **a.** Authenticate Using an AAA Server Group オプション ボタンをクリックします。
 - **b.** 事前設定されているサーバ グループを Authenticate using an AAA Server Group ドロップダウン リストから選択するか、New をクリックして新しい AAA サーバ グループを追加します。

■ IPSec リモートアクセス VPN シナリオの実装

薩 YPN Wizard		×
VPN Wizard	Client Authentication (Step 4 of)	
Branch Branch Branch Home Corporate Notwork	To authenticate remote users using local device user database, select the first option below. You can create user accounts in the next step. To use external AAA servers instead, select the second option. You can select an existing AAA server group or create a new one using the New button below. To manage all other AAA settings, go to Configuration > Device Management > Users/AAA in the main ASDM window.	
	<u>≤Back</u> <u>N</u> ext > <u>E</u> nish <u>Cancel</u> <u>H</u> elp	

ステップ3 Next をクリックして続行します。

(オプション) ユーザ アカウントの設定

ローカル ユーザ データベースを使用してユーザを認証する場合、次の手順で新 しいユーザ アカウントを作成できます。ASDM 設定インターフェイスを使用し て、後でユーザを追加することもできます。

VPN Wizard の Step 5 で、次の手順に従います。

ステップ1 新しいユーザを追加するには、ユーザ名とパスワードを入力し、Add をクリック します。

💕 VPN Wizard	
VPN Wizard	User Accounts (Step 5 of 11)
Brandt	Enter a new username/password into the user authentication database. To edit existing entries in the database or to remove them from the database, go to Configuration > Properties > Device Administration > User Accounts in the main ASDM window.
Home	User to Be Added
Corporate Network	Username: Add >>
	Password (optional): Delete
	Confirm Password (optional):
	< Back Next > Finish Cancel Help

ステップ2 新しいユーザの追加が終了したら、Next をクリックして続行します。

Cisco ASA 5505 クイック スタート ガイド

アドレス プールの設定

リモート クライアントがネットワークにアクセスするには、接続に成功したときにリモート VPN クライアントに割り当てられる可能性のある IP アドレスの プールを設定する必要があります。このシナリオでは、プールは 209.165.201.1 ~ 209.166.201.20 の範囲の IP アドレスを使用するように設定します。

VPN Wizard の Step 6 で、次の手順に従います。

ステップ1 プール名を入力するか、事前設定されているプールを Name ドロップダウン リ ストから選択します。

または、New をクリックして、新しいアドレス プールを作成します。

Add IP Pool ダイアログボックスが表示されます。

🖆 Add IP Pool	×
Name:	RemoteClientPool
Starting IP Address:	209.165.201.1
Ending IP Address:	209.165.201.20
Subnet Mask:	· · · · · · · · · · · · · · · · · · ·
ок	Cancel Help

ステップ2 Add IP Pool ダイアログボックスで、次の内容を実行します。

- a. 範囲の開始 IP アドレスと終了 IP アドレスを入力します。
- **b.** (オプション) サブネット マスクを入力するか、Subnet Mask ドロップダウ ンリストから IP アドレス範囲のサブネットマスクを選択します。
- **c.** OK をクリックして、VPN Wizard の Step 6 に戻ります。

💕 VPN Wizard	
VPN Wizard	Address Pool (Step 6 of 11)
Brandt	Enter a pool of local addresses to be used for assigning dynamic IP addresses to remote VPN clients.
Corporate Network	Tunnel Group Name : Cisco
THE IN	Pool Name: RemoteClientPool V New
	Pool Settings Range Start Address: 209.165.201.1
T	Range End Address: 209.165.201.20
	Subnet Mask:
	< Back Next > Finish Cancel Help

ステップ3 Next をクリックして続行します。

クライアント アトリビュートの設定

各リモート アクセス クライアントがネットワークにアクセスするには、使用す る DNS サーバと WINS サーバ、デフォルトのドメイン名などの基本的なネット ワーク設定情報が必要です。各リモート クライアントを個々に設定するのでは なく、ASDM にクライアント情報を設定できます。接続が確立されると、適応 型セキュリティ アプライアンスは、この情報をリモート クライアントまたは Easy VPN ハードウェア クライアントに適用します。

必ず正しい値を指定してください。値が正しくない場合、リモート クライアン トが解決に DNS 名を使用できない、または Windows ネットワーキングを使用で きないという問題が発生します。

VPN Wizard の Step 7 で、次の手順に従います。

ステップ1 リモート クライアントに適用するネットワーク設定情報を入力します。

🖆 VPN Wizard		
VPN Wizard	Attributes Pushed to Client (Optional) (Step	17 of 11)
Branch	Attributes you configure below are pushed ASA. If you do not want an attribute pushed	to the VPN client when the client connects to the I to the client, leave the corresponding field blank.
Corporate Corporate	Tunnel Group: Ci	sco
Net	Primary DNS Server:	209.165.205.129
	Secondary DNS Server:	2þ9.165.202.139
	Primary WINS Server:	209.165.202.118
- LI	Secondary WINS Server:	209.165.202.168
	Default Domain Name:	cisco.com
		< Back Next > Finish Cancel Help

ステップ2 Next をクリックして続行します。

IKE ポリシーの設定

IKE は、データを保護しプライバシーを保証する暗号化方式を含むネゴシエー ションプロトコルで、ピアの ID を確認する認証方式でもあります。ほとんどの 場合、ASDM のデフォルト値を使用すれば、十分にセキュアな VPN トンネルを 確立できます。

VPN Wizard の Step 8 で IKE ポリシーを指定するには、次の手順に従います。

ステップ1 IKE セキュリティ アソシエーションにおいて適応型セキュリティ アプライアン スが使用する暗号化アルゴリズム (DES、3DES、または AES)、認証アルゴリズ ム (MD5 または SHA)、および Diffie-Hellman グループ (1、2、5、または 7)を 選択します。

🖆 VPN Wizard		
VPN Wizard	IKE Policy (Step 8 of 11)	
Brendt Brendt Brendt Brendt Brendt Brendt Brendt Brendt	Select the encryption algorithm, authentication algorithm, and Diffie-Hellman group for the devices to use to negotiate an Internet Key Exchange (IKE) security association between them. Configurations on both sides of the connection must match exactly.	
Corporate	Encryption: 3DES	
	DH Group: 2	
	< Back Next > Finish Cancel Help	

ステップ2 Next をクリックして続行します。

IPSec Encryption パラメータ および Authentication パラメータの設定

VPN Wizard の Step 9 で、次の手順に従います。

ステップ1 暗号化アルゴリズム (DES、3DES、または AES) および認証アルゴリズム (MD5 または SHA) をクリックします。

薩 VPN Wizard		×
VPN Wizard	IPsec Encryption and Authentication (Step 9 of 11)	
Brench ISP Corporate	Select the encryption and authentication algorithms for this IPsec VPN tunnel. Configurations on both sides of the connection must match exactly.	
Network	Encryption:	
	Authentication: SHA	
	<u>≤ Back</u> <u>N</u> ext > Einish <u>C</u> ancel <u>H</u> el	153919

ステップ2 Next をクリックして続行します。

アドレス変換の例外およびスプリット トンネリングの指定

スプリット トンネリングを使用すると、リモートアクセス IPSec クライアント は、パケットを条件によって、IPSec トンネル経由で送信すること(暗号化形式) や、ネットワーク インターフェイスに送信すること(テキスト形式)ができます。

適応型セキュリティアプライアンスは、Network Address Translation (NAT; ネットワークアドレス変換)を使用して、内部 IP アドレスが外部に公開されないようにしています。認証されたリモート ユーザにアクセスを許可するローカル ホストおよびネットワークを特定することで、このネットワーク保護に例外を設定できます。

VPN Wizard の Step 10 で、次の手順に従います。

ステップ1 認証されたリモート ユーザにアクセスを許可する内部リソースのリストに入れ るホスト、グループ、およびネットワークを指定します。

> Selected Hosts/Networks ペインのホスト、グループ、およびネットワークを動的 に追加するには Add、動的に削除するには Delete をクリックします。

🞼 YPN Wizard	X
VPN Wizard	Address Translation Exemption and Split Tunneling (Optional) (Step 10 of 11)
Branch Branch ISP Home	Network Address Translation (NAT) is used to hide the internal network from outside users. You can make exceptions to NAT to expose the entire or part of the internal network to authenticated remote users protected by VPN. To expose the entire network behind the most secure interface to remote VPN users without NAT, leave the selection list blank.
Corporate Network	Host/Network 10.10.10.0
	Interface: inside Add Address: 10.10.10.0 Delete
	Enable split tunneling to let remote users have simultaneous encrypted access to the resources defined above, and unencrypted access to the internet.
	<u>≤ Back</u> <u>N</u> ext > <u>Einish</u> <u>Cancel</u> <u>H</u> elp



画面下部の Enable Split Tunneling … チェックボックスをオンにすると、 スプリットトンネリングがイネーブルになります。スプリットトンネリングを使用すると、設定したネットワークの外部のトラフィックは、暗 号化された VPNトンネルを経由せずにインターネットに直接送信され ます。

ステップ2 Next をクリックして続行します。

リモートアクセス VPN 設定の確認

VPN Wizard の Step 11 で、新しい VPN トンネルの設定アトリビュートを確認します。表示される設定は次のようになります。



適切に設定されている場合は Finish をクリックして、適応型セキュリティ アプ ライアンスに変更内容を適用します。

次にデバイスを起動するときに適用されるように、設定変更をスタートアップ コンフィギュレーションに保存する場合は、File メニューから Save をクリック します。または、ASDM を終了するときに設定変更を半永久的に保存するよう に求められます。 設定変更を保存しない場合は、次にデバイスを起動するときに変更前の設定がそ のまま適用されます。

次の作業

モバイル従業員またはテレワーカー向けの安全な接続用にエンドツーエンドの 暗号化 VPN トンネルを確立するには、Cisco VPN クライアント ソフトウェアを 入手します。

Cisco Systems VPN クライアントの詳細については、

http://www.cisco.com/en/US/products/sw/secursw/ps2308/index.html を参照してください。

リモートアクセス VPN 環境だけに適応型セキュリティアプライアンスを配置す る場合は、これで初期設定が終了しました。さらに、次の手順を実行することも できます。

実行内容	参照先
詳細な設定およびオプション機	\llbracket Cisco Security Appliance Command Line
能と拡張機能の設定	Configuration Guide.
日常的な運用について	$\llbracket Cisco \ Security \ Appliance \ Command \ Reference rbrace$
	Cisco Security Appliance Logging Configuration and System Log Messages

複数のアプリケーションに適応型セキュリティ アプライアンスを設定できま す。次の項では、適応型セキュリティアプライアンスの他の一般的なアプリケー ションの設定手順について説明します。

実行内容	参照先
DMZ 内の Web サーバを保護するため	第6章「シナリオ:DMZ 設定」
の適応型セキュリティ アプライアン	
スの設定	
サイトツーサイト VPN の設定	第8章「シナリオ:サイトツーサイト
	VPN 設定」